UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/615,490 | 07/07/2003 | Nicolas Cerf | VANM256.001AUS | 8981 |

20995 7590 06/05/2007
KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

| EXAMINER | |
|---|---|
| DAVIS, ZACHARY A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 06/05/2007 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

jcartee@kmob.com
eOAPilot@kmob.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/615,490 | CERF ET AL. | |
| | Examiner | Art Unit | |
| | Zachary A. Davis | 2137 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *06 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06 March 2007 has been entered.

2. By the above submission, Claims 7, 14, 17, and 20 have been amended. New Claims 30-32 have been added. No claims have been canceled. Claims 1-32 are currently pending in the present application.

### *Response to Arguments*

3. Applicant's arguments with respect to claims 1-29 have been considered but are moot in view of the new ground(s) of rejection.

**_Response to Amendment_**

4. The declaration under 37 CFR 1.132 filed 06 March 2007 is insufficient to overcome the rejection of claims 1-29 based upon 35 U.S.C. 102(e) as anticipated by Nambu, US Patent 6801626, as set forth in the last Office action because:

The evidence presented in the declaration, and specifically in paragraph 4 of the declaration (pages 2-3 of the declaration), is opinion testimony, as explicitly stated. Although factual evidence is preferable to opinion testimony, such testimony is entitled to consideration and some weight so long as the opinion is not on the ultimate legal conclusion at issue. While an opinion as to a legal conclusion is not entitled to any weight, the underlying basis for the opinion may be persuasive. *In re Chilowsky*, 306 F.2d 908, 134 USPQ 515 (CCPA 1962); *In re Lindell*, 385 F.2d 453, 155 USPQ 521 (CCPA 1967). See MPEP § 716.01(c) III.

Further, it is noted that it is uncommon to submit a declaration under 37 CFR 1.132 traversing an anticipation rejection under 35 U.S.C. 102, and that such declarations are more commonly submitted in situations showing secondary considerations for a determination of obviousness under 35 U.S.C. 103 or whether there is sufficient disclosure under 35 U.S.C. 112, first paragraph.

However, it is further noted that the above is moot in view of the new ground(s) of rejection.

***Claim Objections***

5. Claims 14-17, 20, 22, and 26 are objected to because of the following informalities:

In Claim 14, in the limitation "converting the resulting raw key which is in the form of a set of correlated Gaussian variables into a binary secret key", it appears that commas should be inserted between "key" and "which", and between "variables" and "into".

In Claim 15, in line 7 of the claim, it appears that "reconciliating" is intended to read "reconciling".

In Claim 16, in line 2 of the claim, it appears that "reconciliated" is intended to read "reconciled".

In Claim 17, in line 12 of the claim, it appears that "used to communicating" is intended to read "used to communicate".

In Claim 20, line 2, it appears that a comma should be inserted between "parties" and "which".

In Claim 22, line 2, it appears that "comprised" should be deleted.

In Claim 26, line 1, it appears that "additional" is intended to read "additionally".

Appropriate correction is required.

### *Claim Rejections - 35 USC § 112*

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-32 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitations "the sending unit" and "the receiving unit" in line 9 of the claim. Because the claim initially recites that there is "at least one sending unit" and "at least one receiving unit", if there is more than one of these units, it is not clear to which of these units "the sending unit" and/or "the receiving unit" is intended to refer.

Claim 3 recites the limitation "the sent and received raw data resulting from the continuous-variable protocol". There appears to be insufficient antecedent basis for this limitation in the claims.

Claim 4 recites the limitation "high signal-to-noise ratio". The term "high" is a relative term that is not clearly defined in the claims or specification, nor is there a standard of comparison provided. See MPEP § 2173.05(b). Further, the claim recites the limitation "several key bits". The term "several" is generally vague and indefinite because it does not refer to a specific number, quantity, or numerical range. Further, the term is not clearly defined in the specification or claims, nor is a clear standard of comparison provided.

Claim 5 recites the limitation "high secret bit rates in comparison to photon-counting techniques". The use of the relative term "high" renders the claim indefinite because it is not clearly defined. Although a standard of comparison is provided, this is not a fixed standard, since such techniques could conceivably improve beyond the known range implied by the present specification. See MPEP § 2173.05(b).

Claims 6 and 7 recite the limitations "low losses" and "high losses" respectively. The use of the relative terms "low" and "high" renders the claims indefinite, because the terms are not clearly defined in the claims or specification, and there is no clear standard of comparison provided. See MPEP § 2173.05(b).

Claim 12 recites the limitation "pulses typically containing several photons". The use of the term "typically" does not clearly further limit the parent claim, because it does not clearly describe the situation in which atypical pulses may be present. Further, the use of the term "several" is generally vague and indefinite because it does not refer to a specific number, quantity, or numerical range. Further, the term is not clearly defined in the specification or claims, nor is a clear standard of comparison provided.

Claim 14 recites the limitation "the wrong one" in line 9 of the claim. This term is generally vague, although it appears to refer the one of quadrature x or p that was not measured in the step at lines 6-7 of the claim. The claim further recites the limitation "converting the resulting raw key which is in the form of a set of correlated Gaussian variables into a binary secret key comprising direct or reverse reconciliation in order to correct the errors and get a binary key, and privacy amplification in order to make secret the binary key". This limitation is generally unclear. Specifically, it is not clear what the

subject of the verb "comprising" is; although, from the language of the claim, it appears that the "binary secret key" is what comprises direct or reverse reconciliation, it is not clear how the key can include the claimed reconciliation. Further, it is not clear what the phrase beginning "privacy amplification" modifies, or of what the privacy amplification is the (grammatical) object.

Claim 15 recites the limitation "wherein the reconciliation produces a common bit string from correlated continuous data, which comprises the following". Although it appears that the term "which" is intended to refer to the "correlated continuous data" given the placement of the phrases, it is not clear how data includes the elements of transforming, converting, and "reconciliating [sic]".

Claim 17 recites the limitations "high repetition rate", "high frequency", and "high acquisition frequency". The use of the relative term "high" renders the claim indefinite, because the term is not clearly defined in the claims or specification, and there is no clear standard of comparison provided. See MPEP § 2173.05(b).

Claim 18 recites the limitation "a local oscillator is transmitted". This is generally unclear, although it appears that this is intended to describe a signal, generated by a local oscillator, that is transmitted. Further, the claim recites the limitations "a strong local oscillator pulse" and "a weak orthogonally-polarized signal pulse". The use of the relative terms "strong" and "weak" renders the claim indefinite, because the terms are not clearly defined in the claims or specification, and there is no clear standard of comparison provided. See MPEP § 2173.05(b).

Claim 20 recites the limitation “several photons”. The term “several” is generally vague and indefinite because it does not refer to a specific number, quantity, or numerical range. Further, the term is not clearly defined in the specification or claims, nor is a clear standard of comparison provided. Further, the claim has been amended to recite the limitation “each pulse typically containing several photons and is continuously modulated in phase and amplitude”. It is not clear what the subject of the phrase “is modulated in phase and amplitude” is.

Claim 21 recites the limitation “the post-processing protocols”. There is insufficient antecedent basis for this limitation in the claims.

Claim 26 recites the limitation “the wrong one” in line 10 of the claim. This term is generally vague, although it appears to refer the one of quadrature x or p that was not measured in the step at lines 7-8 of the claim. The claim further recites the limitation “means for converting the resulting raw key in the form of a set of correlated Gaussian variables into a binary secret key comprising direct or reverse reconciliation in order to correct the errors and get a binary key, and privacy amplification in order to make secret the binary key”. This limitation is generally unclear. Specifically, it is not clear what the subject of the verb “comprising” is; although, from the language of the claim, it appears that the “binary secret key” is what comprises direct or reverse reconciliation, it is not clear how the key can include the claimed reconciliation. Further, it is not clear what the phrase beginning “privacy amplification” modifies, or of what the privacy amplification is the (grammatical) object.

Claim 28 recites "The method of Claim 17"; however, Claim 17 is directed to a device. Claim 28 also recites the limitation "high repetition rate"; the use of the relative term "high" renders the claim indefinite, because the term is not clearly defined in the claims or specification, and there is no clear standard of comparison provided. See MPEP § 2173.05(b). The claim further recites the limitation "many photons". The term "many" is generally vague and indefinite because it does not refer to a specific number, quantity, or numerical range. Further, the term is not clearly defined in the specification or claims, nor is a clear standard of comparison provided.

Claim 29 recites the limitation "several photons". The term "several" is generally vague and indefinite because it does not refer to a specific number, quantity, or numerical range. Further, the term is not clearly defined in the specification or claims, nor is a clear standard of comparison provided.

Claim 30 recites the limitation "wherein numbers from a continuous distribution are encoded". However, this is somewhat unclear, as the claim is directed to a system and it is not clear which entity in the system performs the claimed encoding.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nambu, US Patent 6801626, in view of Ralph, "Continuous variable quantum cryptography" (cited by Applicant on the information disclosure statement received 15 December 2003).

In reference to Claim 1, Nambu discloses a quantum cryptographic system including a sending unit including an encoder for distributing a raw key in the quadrature components of quantum coherent states (abstract; col. 1, lines 14-48; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 44); a receiving unit including a homodyne detector of the quantum coherent states in order to measure the quadrature components of the states (abstract; col. 1, lines 14-48; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53); a quantum channel for connecting the sending unit to the receiving unit (col. 1, lines 14-48); and a two-way authenticated public channel for transmitting non-secret messages between the sending unit and the receiving unit (col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53). However, Nambu does not explicitly disclose that the quantum states are continuously modulated in phase and amplitude.

Ralph discloses a system for continuous variable quantum cryptography, in which phase and amplitude are continuously modulated (see Figure 1, for example; also note page 1, left column). Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Nambu to include the use of continuously modulated phase and amplitude quadrature values, in order to gain the benefits of equivalent

security to single-photon models (see Ralph, page 1, right column) without the disadvantages of working with single photons (see Ralph, page 1, left column).

In reference to Claim 2, Nambu and Ralph further disclose a continuous-variable quantum key distribution protocol ensuring that the amount of information a potential eavesdropper may gain at most on the sent and received data can be estimated from the measured parameters of the quantum channel (error rate and line attenuation) (Nambu, col. 1, lines 14-48; col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53; see also Ralph).

In reference to Claim 3, Nambu and Ralph further disclose that sent and received raw data resulting from the continuous-variable protocol are converted into a secret binary key by using a continuous reconciliation protocol supplemented with privacy amplification (Nambu, col. 1, lines 14-48; col. 2, lines 32-57; col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53).

In reference to Claim 6, Nambu and Ralph further disclose that the continuous reconciliation protocol is a direct reconciliation protocol, which allows the receiver to discretize and correct its data according to the sent values, in case of noisy quantum channels with low losses (Nambu, col. 1, lines 14-48; col. 4, lines 4-42; col. 2, lines 32-57).

In reference to Claim 7, Nambu and Ralph further disclose that the continuous reconciliation protocol is a reverse reconciliation protocol, which allows the sending unit to discretize and correct its data according to the values measured by the receiver, in

case of noisy quantum channels with high losses (Nambu, col. 1, lines 14-48; col. 4, lines 4-42; col. 2, lines 32-57).

In reference to Claim 8, Nambu and Ralph further disclose that the secret key is used as a private key for ensuring confidentiality and authentication of a cryptographic transmission (Nambu, col. 2, lines 32-57).

In reference to Claim 4, Nambu and Ralph further disclose that the encoder of the quadrature components with a high signal-to-noise ratio encodes multiple key bits per coherent light pulse (Nambu, col. 4, lines 4-42; col. 4, line 63 – col. 5, line 53; see also Ralph).

In reference to Claim 5, Nambu and Ralph further disclose that the decoding of the quadrature components of the light field via the homodyne detector achieves high secret bit rates in comparison to photon-counting techniques (Nambu, col. 4, line 63 – col. 5, line 53).

In reference to Claim 9, Nambu and Ralph further disclose that the quadrature components of the quantum coherent states are modulated with a Gaussian distribution (Nambu, col. 9, line 60 – col. 11, line 12).

In reference to Claim 10, Nambu and Ralph further disclose that the co-ordinate values of the center of the Gaussian distribution are arbitrary (Nambu, col. 9, line 60 – col. 11, line 12).

In reference to Claim 11, Nambu and Ralph further disclose that the variance of the Gaussian distribution for the quadrature X is different from the variance of the

Gaussian distribution for the conjugate quadrature P (Nambu, col. 9, line 60 – col. 11, line 12).

In reference to Claim 12, Nambu and Ralph further disclose that the Gaussian-modulated coherent states are attenuated laser light pulses typically containing multiple photons (Nambu, abstract; col. 4, line 63 – col. 5, line 53; col. 9, line 60 – col. 11, line 12).

In reference to Claim 13, Nambu and Ralph further disclose that the information an eavesdropper may gain on the sent and received Gaussian-distributed values are calculated explicitly using Shannon's theory for Gaussian channels (Nambu, col. 2, line 32-57; col. 6, line 34 – col. 7, line 6; col. 9, line 60 – col. 11, line 12).

In reference to Claim 30, Nambu and Ralph further disclose numbers from a continuous distribution encoded into corresponding phase shifts and amplitudes (see Ralph, page 1, left and right columns, for example).

In reference to Claim 14, Nambu discloses a method of distributing continuous quantum key between a sender and a receiver, where the method includes selecting, at a sender, two random numbers $x_A$ and $p_A$ from a Gaussian distribution of mean zero and variance $V_A N_0$, where $N_0$ refers to the shot-noise variance (col. 9, line 60 – col. 11, line 12); sending a corresponding coherent state $|x_A + ip_A>$ in the quantum channel (col. 4, line 63 – col. 5, line 53); randomly choosing, at a receiver, to measure either quadrature x or p using homodyne detection (col. 4, line 63 – col. 5, line 53; col. 6, line 34 – col. 7, line 6; col. 9, lines 36-59); informing the sender about the quadrature that

was measured so the sender may discard the quadrature that was not measured (col. 2, lines 32-57); measuring channel parameters on a random subset of the sender's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper (col. 2, lines 32-57; col. 4, lines 4-42); and converting the resulting raw key in the form of a set of correlated Gaussian variables into a binary secret key, by using direct or reverse reconciliation in order to correct the errors and get a binary key and privacy amplification in order to make secret the binary key (col. 2, lines 32-57; col. 4, lines 4-42; col. 9, line 60 – col. 11, line 12). However, although Nambu does disclose the modulating phase as noted above, Nambu does not explicitly disclose that the quantum states are continuously modulated in both phase and amplitude.

Ralph discloses a system for continuous variable quantum cryptography, in which phase and amplitude are continuously modulated (see Figure 1, for example; also note page 1, left column). Therefore, it would have been obvious to one of ordinary skill in the art to modify the method of Nambu to include the use of continuously modulated phase and amplitude quadrature values, in order to gain the benefits of equivalent security to single-photon models (see Ralph, page 1, right column) without the disadvantages of working with single photons (see Ralph, page 1, left column).

In reference to Claim 15, Nambu and Ralph further disclose that the reconciliation produces a common bit string from correlated continuous data, and that the method further includes transforming each Gaussian key element of a block of size n by the sender into a string of m bits, giving m bit strings of length n, referred to as slices (Nambu, col. 4, line 63 – col. 5, line 53; col. 9, line 60 – col. 11, line 12);

converting, by the receiver, the measured key elements into binary strings by using a set of slice estimators (Nambu, col. 4, line 63 – col. 5, line 53; col. 9, lines 36-59); and sequentially reconciling the slices by using an implementation of a binary error correction algorithm, and communicating on the public authenticated channel (Nambu, col. 2, lines 32-57; col. 7, lines 7-14).

In reference to Claim 16, Nambu and Ralph further disclose the post-processing of privacy amplification comprises distilling a secret key out of the reconciled key by use of a random transformation taken in a universal class of hash functions (Nambu, col. 2, lines 32-57; col. 4, lines 4-42).

In reference to Claim 24, Nambu and Ralph further disclose informing the sender comprises utilizing a public authenticated channel by the receiver to inform the sender (Nambu, col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53).

In reference to Claim 25, Nambu and Ralph further discloses the channel parameters include error rate and line attenuation (Nambu, col. 2, lines 10-57; col. 4, lines 4-42; col. 7, lines 7-49).

In reference to Claim 27, Nambu and Ralph further disclose the sending comprises sending the corresponding coherent state $|x_A + ip_A>$ that is continuously modulated in phase and amplitude in the quantum channel (Nambu, abstract; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; see also Ralph, page 1, left and right columns).

In reference to Claim 17, Nambu discloses a device for implementing a continuous-variable quantum key exchange, where the device includes a light source or a source of electromagnetic signals configured to generate short quantum coherent pulses at a high repetition rate (col. 4, line 63 – col. 5, line 53); an optical component configured to modulate the phase of the pulses at a high frequency (col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53); a quantum channel configured to transmit the pulses from an emitter to a receiver (col. 4, line 63 – col. 5, line 53); a system that permits the transmission of a local oscillator from the emitter to the receiver (col. 4, line 63 – col. 5, line 53; col. 7, lines 7-49); a homodyne detector capable of measuring, at a high acquisition frequency, any quadrature component of the electromagnetic field collected at the receiver's station (col. 4, line 63 – col. 5, line 53); a two-way authenticated public channel that is used to communicate non-secret messages in postprocessing protocols (col. 1, lines 14-48; col. 4, line 63 – col. 5, line 53); and a computer at the emitter's and receiver's stations that drives or reads the optical components and runs the postprocessing protocols (col. 4, line 63 – col. 5, line 53; col. 8, line 39 – col. 9, line 59). However, although Nambu does disclose the modulating phase as noted above, Nambu does not explicitly disclose that the quantum states are continuously modulated in both phase and amplitude.

Ralph discloses a system for continuous variable quantum cryptography, in which phase and amplitude are continuously modulated (see Figure 1, for example; also note page 1, left column). Therefore, it would have been obvious to one of ordinary skill in the art to modify the device of Nambu to include the use of continuously modulated

phase and amplitude quadrature values, in order to gain the benefits of equivalent security to single-photon models (see Ralph, page 1, right column) without the disadvantages of working with single photons (see Ralph, page 1, left column).

In reference to Claim 18, Nambu and Ralph further disclose that a signal from a local oscillator is transmitted together with the signal by use of a polarization encoding system whereby each pulse comprises a strong local oscillator pulse and a weak orthogonally-polarized signal pulse with modulated amplitude and phase (Nambu, col. 2, lines 10-31; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; see also Ralph).

In reference to Claim 19, Nambu and Ralph further disclose that if polarization encoding is used, the receiving system relies on polarization-mode homodyne detection requiring a quarter-wave plate and a polarizing beam splitter (Nambu, col. 2, lines 10-31; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; Ralph, page 2, right column, last paragraph).

In reference to Claim 26, Nambu and Ralph further disclose means for selecting, at the emitter, two random numbers $x_A$ and $p_A$ from a Gaussian distribution of mean zero and variance $V_A N_0$, where $N_0$ refers to the shot-noise variance (Nambu, col. 9, line 60 – col. 11, line 12); means for sending a corresponding coherent state $|x_A + ip_A>$ in the quantum channel (Nambu, col. 4, line 63 – col. 5, line 53); means for randomly choosing, at the receiver, to measure either quadrature x or p using homodyne detection (Nambu, col. 4, line 63 – col. 5, line 53; col. 6, line 34 – col. 7, line 6; col. 9, lines 36-59); means for informing the emitter about the quadrature that was measured so the emitter may discard the quadrature not measured (Nambu, col. 2, lines 32-57);

means for measuring channel parameters on a random subset of the emitter's and receiver's data, in order to evaluate the maximum information acquired by an eavesdropper (Nambu, col. 2, lines 32-57; col. 4, lines 4-42); and means for converting the resulting raw key in the form of a set of correlated Gaussian variables into a binary secret key using direct or reverse reconciliation in order to correct the errors and get a binary key and privacy amplification in order to make secret the binary key (Nambu, col. 2, lines 32-57; col. 4, lines 4-42; col. 9, line 60 – col. 11, line 12).

In reference to Claim 28, Nambu and Ralph further disclose the light source or the source of electromagnetic signals comprises the light source or the source of electromagnetic signals configured to generate, at a high repetition rate, short quantum coherent light pulses that contain many photons and are continuously modulated in phase and amplitude (Nambu, abstract; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; Ralph, page 1, left and right columns).

In reference to Claim 31, Nambu and Ralph further disclose that the pulses represent a pair of numbers selected from a continuous distribution and the quadrature component of the received electromagnetic field is also a number selected from a continuous distribution (see Ralph, page 1, left and right columns).

In reference to Claim 20, Nambu discloses a device for exchanging Gaussian key elements between a sender and a receiver, where the device includes a laser diode associated with a grating-extended external cavity, the laser diode configured to send light pulses at a high repetition rate, each pulse containing multiple photons (col. 4, line

63 – col. 5, line 53; col. 7, lines 7-28); an integrated electro-optic amplitude modulator and a piezoelectric phase modulator, configured to generate randomly-modulated light pulses, the data being organized in bursts of pulses (col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; col. 7, lines 7-28); a beam-splitter to separate the quantum signal from a local oscillator (col. 8, line 39 – col. 9, line 22); and a homodyne detector combining the quantum signal and local oscillator pulses in order to measure one of the two quadrature components of the light field (col. 8, line 39 – col. 9, line 22). However, Nambu does not explicitly disclose that the quantum states are continuously modulated in phase and amplitude.

Ralph discloses a system for continuous variable quantum cryptography, in which phase and amplitude are continuously modulated (see Figure 1, for example; also note page 1, left column). Therefore, it would have been obvious to one of ordinary skill in the art to modify the device of Nambu to include the use of continuously modulated phase and amplitude quadrature values, in order to gain the benefits of equivalent security to single-photon models (see Ralph, page 1, right column) without the disadvantages of working with single photons (see Ralph, page 1, left column).

In reference to Claim 21, Nambu and Ralph further disclose an acquisition board and a computer on the sender's and receiver's sides in order to run post-processing protocols (Nambu, col. 4, line 63 – col. 5, line 53; col. 8, line 39 – col. 9, line 59).

In reference to Claim 22, Nambu and Ralph further disclose that the laser operates at a wavelength between about 700 and about 1600 nm (Nambu, col. 7, lines 7-28).

In reference to Claim 23, Nambu and Ralph further disclose that the laser operates at a telecom wavelength between about 1540 and about 1580 nm (Nambu, col. 7, lines 7-28).

In reference to Claim 29, Nambu and Ralph further disclose that each light pulse sent by the laser diode contains multiple photons and is continuously modulated in phase and amplitude (Nambu, abstract; col. 3, lines 24-65; col. 4, line 63 – col. 5, line 53; col. 7, lines 7-28; Ralph, page 1, left and right columns).

In reference to Claim 32, Nambu and Ralph further disclose that the pulses represent a pair of numbers selected from a continuous distribution and the quadrature component of the measured light field is also a number selected from a continuous distribution (see Ralph, page 1, left and right columns).

## *Conclusion*

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Kimble et al, US Patent 5339182, discusses the use of continuous variables in relation to quantum communications.

b. Lo et al, US Patent Application Publication 2004/0141618, discloses a quantum key system in which continuous variables may be implemented.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER